

EXHIBIT F



Federal Communications Commission
Washington, D.C. 20554

January 29, 2018

Christina Koningisor
Legal Department
New York Times Company
620 8th Avenue
New York, NY

Re: FOIA Control No. 2017-764

Dear Ms. Koningisor:

This letter supplements the response Mr. Nicholas Confessore received from the Federal Communications Commission (the Commission) to the above-captioned FOIA request on July 21, 2017.¹ This supplemental response provides a more detailed explanation for the Commission's denial of Mr. Confessore's request and addresses issues that have been raised in subsequent telephone conversations and written correspondence between the Commission's Office of General Counsel and the Legal Department of The New York Times.

The request Mr. Confessore originally submitted on June 22, 2017, asked for the web server logs for public comments filed between April 26, 2017, and June 7, 2017, in the Commission's "Restoring Internet Freedom" (RIF) docket (Docket No. 17-108). The request also specified particular categories of request and response information contained in these logs.

I. Exemption 6 – Personal Information

The Commission's July 21 response withheld the requested materials under FOIA Exemption 6.² Exemption 6 protects "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."³ Balancing the public's interest in disclosure against each individual commenter's right to privacy, we determined that release of the logs would constitute a clearly unwarranted invasion of personal privacy.

¹ See letter from Christine Calvosa, Deputy Chief Information Officer, FCC, to Nicholas Confessore (July 21, 2017).

² 5 U.S.C. § 552(b)(6).

³ The Supreme Court has interpreted the term "similar files" broadly, to include all information that "applies to a particular individual." *Dep't of State v. Washington Post Co.*, 465 U.S. 595, 602 (1982).

Specifically, the server logs requested by Mr. Confessore document the millions of page requests that the Commission's Electronic Comment Filing System (ECFS) received during a high-traffic period.⁴ These logs contain information about each request, including the Internet Protocol (IP) address from which the request originated.⁵ As the Commission has publicly acknowledged,⁶ some of the requests made to the ECFS servers during this period came from cloud-based automated "bots," but a large number came from human users who accessed the site to submit or review comments in the RIF proceeding. We therefore have reason to believe that many of the IP addresses in these logs are linkable to ECFS commenters and qualify as personally identifiable information.⁷ While the ECFS web page informs commenters that the information they submit to the system will be publicly available via the web,⁸ it does not inform commenters that the IP address information associated with their ECFS sessions will be publicly disclosed.

Accordingly, we have determined that it is reasonably foreseeable that disclosure would harm the privacy interest of the persons mentioned in these records and that Exemption 6 applies.

II. Exemption 7(E) – Information Security

The requested server logs were also withheld under FOIA Exemption 7(E), which protects "records or information compiled for law enforcement purposes [the production of which] would disclose techniques and procedures for law enforcement investigations

⁴ An ECFS query of comments filed in Docket 17-108 yields the result that the Commission received 4,971,885 public comments in this docket between April 26 and June 6, 2017. This number does not include the likely millions of additional ECFS users who accessed the system during this period to conduct searches and make other queries.

⁵ See generally, U.S. Computer Emergency Readiness Team, Department of Homeland Security, "Home Network Security," <https://www.us-cert.gov/Home-Network-Security#II-G>. ("H. What Is an IP address? IP addresses are analogous to telephone numbers -- when you want to call someone on the telephone, you must first know their telephone number. Similarly, when a computer on the Internet needs to send data to another computer, it must first know its IP address. IP addresses are typically shown as four numbers separated by decimal points, or "dots." For example, 10.24.254.3 and 192.168.62.231 are IP addresses...I. What are static and dynamic addressing? Static IP addressing occurs when an ISP permanently assigns one or more IP addresses for each user. These addresses do not change over time...Dynamic IP addressing allows the ISP to efficiently utilize their address space. Using dynamic IP addressing, the IP addresses of individual user computers may change over time. If a dynamic address is not in use, it can be automatically reassigned to another computer as needed.") See *Kortlander v. BLM*, 816 F. Supp. 2d 1001, 1015 (D. Mont. 2011) and *Acosta v. FBI*, 946 F. Supp. 2d 53, 65 (D.D.C. 2013), for cases in which courts have approved of redactions of IP addresses under FOIA exemptions.

⁶ See e.g., Letter from Ajit V. Pai, Chairman, FCC, to U.S. Senator Ron Wyden (June 15, 2017), <https://www.fcc.gov/ecfs/filing/10623112818894>.

⁷ See, e.g., 16 C.F.R. § 312.2 (rules implementing the Children's Online Privacy Protection Act include in the definition of "personal information" persistent identifiers like IP addresses that can be used to recognize a user over time and across different websites or online services); Office of Management and Budget, Circ. A-130, 33 (2016) (defining PII as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.")

⁸ FCC, ECFS, "Submit a Filing," <https://www.fcc.gov/ecfs/filings>.

or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk a circumvention of the law.”⁹ The requested logs would publicly disclose information about how the Commission protects the security of ECFS and its other information assets. In particular, the logs would provide detailed information about the Commission’s relationship with commercial cloud servers and the infrastructure the Commission uses to manage ECFS and protect it from disruptive attacks. In addition to disclosing the security measures the Commission generally takes to protect ECFS, the logs would also disclose detailed information about the steps the FCC took in response to the spike in ECFS traffic during early May, thereby giving future attackers a “roadmap” to evade the Commission’s future defensive efforts.

In light of the foregoing, we have determined that it is reasonably foreseeable that disclosure would allow circumvention of certain infrastructure protection mechanisms, and thus that Exemption 7 applies.

III. Reasonable Segregability

The FOIA requires that “any reasonably segregable portion of a record” must be released after appropriate application of the Act’s exemptions.¹⁰ The statutory standard requires the release of any portion of a record that is nonexempt and that is “reasonably segregable” from the exempt portion. However, when nonexempt information is “inextricably intertwined” with exempt information, reasonable segregation is not possible.¹¹ We have determined that because the volume of the requested server logs is so massive and because the sensitive personal and security information described above is so interspersed with other information in the logs, it is not possible to reasonably segregate the exempt from the non-exempt information.

The server logs that are the subject of the request consist of hundreds of millions of lines of technical information documenting the servers’ activities. Reviewing these logs to redact IP addresses linkable to individuals and information revealing the Commission’s information security practices would require a line-by-line review by personnel with technical expertise and would require hundreds of staff hours. While we note and appreciate your organization’s efforts to narrow the scope of your request,¹² we have

⁹ 5 U.S.C. § 552(b)(7)(E). See *Bigwood v. Dep’t of Defense*, 132 F. Supp. 3d 124, 152 (D.D.C. 2015) (citing *Ctr. for Nat’l Sec. Studies v. Dep’t of Justice*, 331 F.3d 918, 926 (D.C. Cir. 2003)) (“Importantly, the range of ‘law enforcement purposes’ covered by Exemption 7(E) includes not only traditional criminal law enforcement duties, but also proactive steps taken by the government designed to prevent terrorism or maintain national security.”) See also *Levinthal v. Fed. Election Comm.*, 219 F. Supp. 3d 1, 7 (D.D.C. 2016) (“[T]he Commission . . . cannot effectively carry out its law enforcement function unless it has a secure and reliable IT system.”)

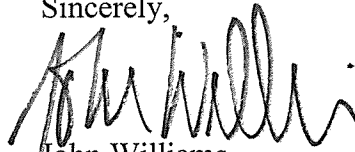
¹⁰ 5 U.S.C. § 552(b) (sentence immediately following exemptions).

¹¹ *Mead Data Cent. Inc. v. Dep’t of the Air Force*, 566 F.2d 242, 260 (D.C. Cir. 1977).

¹² See e.g., Letter from Christina Koningisor, Legal Department, New York Times to John Williams, Senior Counsel to the General Counsel, FCC (Dec. 21, 2017) (proposing to narrow the request to comments filed through both <https://www.fcc.gov/ecfs/filings/> and the Commission’s application programming interface (API) between April 26, 2017, and June 7, 2017 to the following four data elements: comment, originating IP address, date and time stamp, and User-Agent header).

concluded that conducting such a time- and resource-intensive review would be inordinately burdensome.¹³

Sincerely,

A handwritten signature in black ink, appearing to read 'John Williams', written over the printed name.

John Williams
Senior Counselor
Office of the General Counsel

¹³ See *Solar Sources, Inc. v. US*, 142 F.3d 1033, 1039 (7th Cir. 1998) (citing *Lead Indus. Ass'n. v. OSHA*, 610 F.2d 70, 86 (2nd Cir. 1979)) (requiring an agency to review a large number of documents to locate the small number of non-exempt documents within them imposes a burden on the agency and the reviewing courts that conflicts with the “practical approach” courts have taken in interpreting FOIA).